IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff, v. GARY REIBERT, Defendant.	**8:13CR107** **MEMORANDUM AND ORDER**

This matter is before the court on defendant Gary Reibert's objection, Filing No. 350, to the Findings and Recommendation ("F&R") of the United States magistrate judge, Filing No. 347, on Reibert's motion to suppress evidence found in a search of his residence on April 8, 2013.[1] Filing No. 117. Reibert is charged in the Second Superseding Indictment with the receipt and attempted receipt of child pornography (Count I) in violation of 18 U.S.C. § 2252A(a)(2) and (b)(1) and the accessing of a computer in interstate commerce with the intent to view child pornography (Count II) in violation of 18 U.S.C. § 2252A(a)(5)(B) during the period of November 16, 2012, and December 2, 2012. *See* Filing No. 110, second superseding indictment.

In his motion to suppress defendant Reibert challenges two search warrants, one authorizing the government to install a Network Investigation Technique ("NIT") on a seized computer, and one authorizing the search of his residence.

[1] The portion of the defendant's motion challenging the admissibility of his statements was withdrawn at the evidentiary hearing. See Filing No. 330, Transcript at 33-35; Filing No. 347, F&R at 1 n.1. Also, the defendant's challenge to the delayed notice of the warrant was denied after an omnibus evidentiary hearing in an order dated October 14, 2014. *See* Filing No. 294, Memorandum and Order at 7-8, 10.

Defendant Reibert objects to the magistrate judge's F&R, contending he was entitled to a *Franks* hearing[2] on the issue of whether the affidavit in support of the warrant to employ the NIT failed to include evidence that negated probable cause. He also argues the government conducted a warrantless search of Reibert's computer by employing a NIT and contends he was entitled to present testimony of an expert, Tami Loehrs, on this issue. Further, he states the search warrant permitting the NIT was a general warrant and did not permit a search of Reibert's computer, nor was it a warrant authorizing a search of Reibert's computer. Last, he contends the warrant to search Reibert's residence and computer was not based upon probable cause.

Pursuant to 28 U.S.C. § 636(b)(1)(A), the court has conducted a de novo determination of those portions of the F&R to which the defendant objects. *United States v. Lothridge*, 324 F. 3d 599, 600-01 (8th Cir. 2003). The court has reviewed the record, including the transcript of the suppression hearing, and the exhibits. *See* Filing No. 330, Transcript ("Tr."); Filing No. 164, Exs. 1-5; Filing No. 323, Exhibit List. The court accepts the facts set out by the magistrate judge and they need not be repeated here, except to the extent necessary to this court's findings. Filing No. 347, F&R at 2-4; Filing No. 330.[3]

"In order to be entitled to a hearing under *Franks* the defendant must make a substantial preliminary showing of a false or reckless statement or omission and must

---

[2] *See Franks v. Delaware,* 438 U.S. 154, 178 (1978)(holding that, under certain limited circumstances, a defendant is entitled under the Fourth Amendment to collaterally attack the veracity of a warrant affidavit in the context of challenging the existence of probable cause).

[3] *See also* Filing No. 254, F&R at 5-7 (background facts involving government's investigation of "Website A" and the onion router (TOR) software).

also show that the alleged false statement or omission was necessary to the probable cause determination." *United States v. Crissler*, 539 F.3d 831, 833 (8th Cir. 2008) (quoting *United States v. Milton*, 153 F.3d 891, 896 (8th Cir. 1998)). This burden is "not easily [met]." *United States v. Engler*, 521 F.3d 965, 969 (8th Cir. 2008); *see also United States v. Stropes*, 387 F.3d 766, 771 (the defendant must show that the alleged omission would have made it impossible to find probable cause). "[I]f, when material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required." *Franks*, 438 U.S. at 171–72.

The court agrees with the magistrate judge's conclusion that defendant Reibert failed to make the substantial preliminary showing that law enforcement intentionally or recklessly omitted information from the warrant affidavit so as to entitle him to a *Franks* hearing. The defendant argues, in effect, that the government did not disclose in affidavits that it had installed a "trojan, in essence a virus, onto [defendant Reibert's] computer." Filing No. 330, Tr. at 14. The defendant made an offer of proof on the expert testimony it would proffer in support of that contention. *Id.* at 16-28. The court has reviewed the offer of proof and agrees with the magistrate judge that it does not satisfy the heavy burden of showing an intentional falsehood or omission. The court finds no error in the magistrate judge's denial of defendant Reibert's motion for a *Franks* hearing.

Further, the court has reviewed the warrant applications and agrees with the magistrate judge that the warrants were supported by probable cause. *See* Filing No. 164, Index of Evid., Exs. 1 & 2, search warrant applications and affidavits (sealed).

"Probable cause exists when a 'practical, common-sense' inquiry that considers the totality of the circumstances set forth in the information before the issuing judge yields a 'fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Stevens*, 530 F.3d 714, 718 (8th Cir. 2008) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). Reibert contends that the expert testimony of Tami Loehrs, a purported computer forensics expert, would establish that the court-authorized deployment of the NIT constituted a warrantless search of his computer "that went into [the defendant's] house, modified the workings of his computer, in order to send back data to the government." Filing No. 330, Tr. at 4. The magistrate judge sustained the government's objection to the expert's testimony on *Daubert* grounds, but allowed an offer of proof with respect to her testimony.[4] Filing No. 330, Transcript at 19-22, 24-28. The court finds no error in the magistrate judge's *Daubert* ruling. Loehrs conceded that she "had no idea" whether "the investigative technique returned any more information than it was authorized." *Id*. at 27-28. She also conceded that flash applications are present on many websites and flash applications can reveal the IP and user. *Id.* at 28. Even if allowed, her testimony does little to undermine the information contained in the affidavit that supports the NIT warrant.

The magistrate judge found the affidavits of Special Agents Jeffrey Tarpinian and Andrea Kenzig provided probable cause for the searches and the court agrees. *See* F&R at 5-6; Filing No. 164, Index of Evid., Exs. 1 & 2. The affidavit in support of the application for a NIT described the investigation, the TOR network, and target website in detail, including the website's function in advertising and distributing child pornography,

[4] *Daubert v. Merrell Dow Pharmaceuticals, Inc*., 509 U.S 579 (1993).

and also related the types and amount of child pornography available on the site, including sections specific to babies and prepubescent boy and girls. *Id*., Ex. 1 at 12-29. It also described the law enforcement investigation that led investigators to the website. *See* Filing No. 164, Ex. 2 at 9-13, 15-20. It also describes the operation to the NIT. *Id.* at 29-32. The warrant authorized the use of a NIT (computer code) to be deployed on the computer server that operated TOR network "Bulletin Board A," then located at a government facility, in order to obtain information, including IP addresses, from computers accessing images on Bulletin Board A or sending or viewing private messages on Bulletin Board A. *Id.* at 39, 44. The affidavit in support of the residential warrant detailed the investigative techniques used to identify Reibert and connect him to the website. Filing No. 164, Ex. 2, Affidavit at 9-15. The affiant states a person with an IP address issued to Reibert accessed the website at issue and specifies and describes the images that were accessed. *Id*. at 16-20. Those facts, together with the affiant's expertise regarding the characteristics of child pornography consumers, supports a fair probability that child pornography would be found on one or more computers at his residence. *Id.* at 22-26.

In the Eighth Circuit, for the purposes of determining whether probable cause exists to search a computer, an IP address assigned to a specific user at the time illegal internet activity associated with that IP address occurs is a sufficient basis to find a nexus between the unlawful use of the internet at that IP address and a computer possessed by the subscriber assigned the address. *See, e.g., United States v. Stults*, 575 F.3d 834, 843–44 (8th Cir. 2009) (holding that probable cause supported warrant where officers used IP address to identify possessor of child pornography on a file-

sharing network); *United States v. Perrine*, 518 F.3d 1196, 1205–06 (10th Cir. 2008) (upholding probable cause where pornographic images were traced to defendant's residence using IP address); *United States v. Perez*, 484 F.3d 735 (5th Cir. 2007)(the IP address provided "a substantial basis to conclude that evidence of criminal activity" would be found at the defendant's home, even if it did not conclusively link the pornography to the residence); *United States v. Wagers*, 452 F.3d 534, 539 (6th Cir. 2006) (upholding probable cause where suspect was identified as a member of child pornography websites through an IP address assigned to his residence); *United States v. Hay*, 231 F.3d 630, 635–36 (9th Cir. 2000) (finding a substantial basis for magistrate's probable cause determination where images of child pornography were traced to defendant using an IP address).

Further, even if the information submitted to support the issuance of a search warrant did not amount to probable cause, the good faith exception to the exclusionary rule identified in *United States v. Leon*, 468 U.S. 897, 922 (1984), would apply. "Under the *Leon* good-faith exception, disputed evidence will be admitted if it was objectively reasonable for the officer executing a search warrant to have relied in good faith on the judge's determination that there was probable cause to issue the warrant." *United States v. Grant*, 490 F.3d 627, 632 (8th Cir. 2007). Even if the Court were now to conclude here that the affidavit supporting the search warrant did not set forth facts sufficient to demonstrate probable cause to search the computers at defendant Reibert's residence, on the present record, law enforcement's good-faith reliance on the warrants issued by the magistrate judge to search those computers militates against suppressing any evidence obtained in the search. *See Leon*, 468 U.S. at 919–921

(exclusionary rule does not apply "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope").

Accordingly, the court concludes that the defendant's objections to the F&R should be overruled, the magistrate judge's F&R should be adopted and the defendant's motion to suppress should be denied.

IT IS ORDERED:

1. Defendant Reibert's objections to the F&R (Filing No. 350) are overruled.
2. The Findings and Recommendation of the magistrate judge (Filing No. 347) is hereby adopted.
3. Defendant Reibert's motion to suppress (Filing No. 117) is denied.

DATED this 27th day of January, 2015.

BY THE COURT:

s/ Joseph F. Bataillon
Senior United States District Judge